d his

(FILE 'HOME' ENTERED AT 14:27:56 ON 17 JUL 2001)

FILE 'USPATFULL' ENTERED AT 14:28:51 ON 17 JUL 2001

L1	108	S	DC OFFSET CORRECTION
L2	451	S	TIME TRACKING
L3	0	S	L1 AND L2
L4	3134	S	AUTOMATIC GAIN CONTROL CIRCUIT
L5	6	S	L4 AND L1
L6	480	S	(ENCRYPT? OR CIPHER? OR ENCIPHER?)(3A)(RANDOM NUMBER?)
L7	0	S	L6 AND L5
L8	0	S	L6 AND L1
L9	0	S	L6 AND L4
L10	4	S	CDMA AND L6

```
(FILE 'HOME' ENTERED AT 16:59:51 ON 17 JUL 2001)

     FILE 'USPATFULL' ENTERED AT 17:00:04 ON 17 JUL 2001
L1           428 S AGC AND DC OFFSET
L2             0 S AGC CIRCUIT AND DC OFFSET LOOP
L3            20 S L1(P)RANDOM NUMBER?
L4         95520 S CELLULAR OR WIRELESS OR HANDPHONE OR CELLPHONE
L5             3 S L3 AND L4

=>
```

d l5 12 kwic

L5 ANSWER 12 OF 13 USPATFULL
SUMM . . . a device or a person and a device in which the device communicates by a direct connection or by a **wireless** exclusive link, such as an optical or IR link, to a security system that controls and restricts the device's access. . .
SUMM . . . one-way commutative function, generate a key signal that represents the authentication value encrypted as an exponential-modulo function of the generated **random number** signal and that further generates a challenge **signal** that represents a base **signal encrypted** as an exponential-modulo function of the **random number** signal. The system further includes a communication port for transmitting the challenge signal to a party requesting access through the. . .

=> d l5 12 pn

L5 ANSWER 12 OF 13 USPATFULL
PI US 5721779 19980224

d l5 6 kwic

L5 ANSWER 6 OF 6 USPATFULL

DETD . . . with the original vectors defined by points A and D respectively, but further from the origin. As noted previously, an **automatic gain control circuit** may be utilized to control such amplitude variations.

DETD In the preferred embodiment of the present invention, the **DC offset correction** circuitry is utilized as part of a receive channel in a modem such as is illustrated in U.S. patent application. . .

DETD . . . coefficient from coefficient update block 27. The coefficients are updated by the difference error feedback loop for phase, amplitude and **DC offset correction**. The output of EQ/FIR 26 is a complex word W(n) which is multiplied at phase coefficient 34 by a correction. . .

ANSWER 5 OF 6 USPATFULL
SUMM . . . as R/W) circuit in a magnetic recording apparatus generally includes a R/W amplifier 12 connected to a head 10, an **automatic gain control circuit** (AGC) 14 connected to the differential outputs of the amplifier 12 through coupling capacitors C1 and C2, and a detector. . .

SUMM For example, IBM Technical Disclosure Bulletin, Vol. 26, No. 4, Sep. 1983, pp. 2100 to 2103 describes a **DC offset correction** in which a fast DC restore loop including an integrator and two comparators is connected to one of the differential. . .

CLM What is claimed is:

. . . recording apparatus comprising: a head; an amplifier used during a read operation for amplifying a signal read by head; an **automatic gain control circuit** for receiving the output of said amplifier used during a read operation; a coupling capacitor between each input and each output of said amplifier used during a read operation and between each input and each output of said **automatic gain control circuit**; a detector connected to the output of said **automatic gain control circuit**; and means for detecting that the operation is switched from writing to reading; means for making the output of said. . .

. . . circuit having a head, an amplifier used during a read operation for amplifying a signal read by the head, an **automatic gain control circuit** for receiving the output of the amplifier, coupling capacitors between each output of the amplifier used during a read operation and the input of the **automatic gain control circuit**, said method for shortening the recovery time which occurs between writing and reading operations of the read/write head comprising the.

.

. . . circuit further comprising: a head; an amplifier used during a read operation for amplifying a signal read by head; an **automatic gain control circuit** for receiving the output of said amplifier used during a read operation; a coupling capacitor between each input and each output of said amplifier used during a read operation and between each input and each output of said **automatic gain control circuit**; a detector connected to the output of said **automatic gain control circuit**; and means for making the output of said amplifier used during a read operation high impedance for a predetermined time. . .

=> d l5 5 pn

L5 ANSWER 5 OF 6 USPATFULL
PI US 5446601 19950829

d l5 4 kwic

L5 ANSWER 4 OF 6 USPATFULL
TI Dual automatic gain control and **DC offset correction** circuit for QAM demodulation
AB A circuit arrangement capable of achieving both **DC offset correction** and automatic gain control for QAM demodulation. The QAM signal is digitized and then the positive signal samples are averaged. . .
SUMM A still further object of the invention is to provide a circuit arrangement capable of achieve both **DC offset correction** and automatic gain control for QAM demodulation.
DETD FIG. 7 shows a block diagram of a combined **DC offset correction** and **automatic gain control circuit**. The circuit of FIG. 7 is essentially a combination of the circuits of FIGS. 4 and 6, and as such,. . .

=> d l5 4 pn

L5 ANSWER 4 OF 6 USPATFULL
PI US 5761251 19980602

d l5 3 kwic

L5 ANSWER 3 OF 3 USPATFULL

SUMM . . . field of radio communication, and more specifically, to the field of output power control in code division multiple access (CDMA) **cellular** telephones.

SUMM Several industry standard publications currently direct design and operation of all types of CDMA **cellular** telephones, including portable mobile stations, handheld mobile stations, and mobile stations mounted in automobiles. These standards are considered to be. . . invention. Standard specifications relevant to the present invention include TIA/EIA/IS-95 Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum **Cellular** System, sections 6.1.1.1-6.1.2.4.2, and TIA/EIA/IS-98, Recommended Minimum Performance Standards for Dual-Mode Wideband Spread Spectrum **Cellular** Mobile Stations, sections 1.4, 10.4.4.1-10.5.2.3.

SUMM Precise mobile station power control is a very important requirement for proper and efficient operation of a CDMA **cellular** telephone system. During times when a mobile station is located far away from the nearest base station, the mobile station. . . necessary to maintain a strong communication link at all times is a requirement to ensure proper operation of a CDMA **cellular** telephone system.

DETD . . . several views, FIG. 1 shows a block diagram representation of portions of a code division multiple access (CDMA) spread spectrum **cellular** radio telephone in accordance with a first preferred embodiment of the present invention. Selected receiver and transmitter circuital elements are. . . IF filtering, baseband signal quadrature splitting and combining, baseband analog to digital and digital to analog conversion, baseband direct current (**DC**) **offset** control, local oscillator quadrature generation, and dock amplitude adjustments. Further in accordance with the first preferred embodiment of the present. . . viterbi decoder and data quality verfication means; and the interleaving/deinterleaving unit includes a convolutional encoder, an interleaver, a deinterleaver, a psuedo-**random** **number** (PN) sequence spreader, a data burst randomizer, and a finite impulse response (FIR) filter. In addition to customary memory and. . .

DETD . . . be understood that the portions of the radio telephone shown in FIG. 1 are only selected parts of the total **cellular** telephone which includes a host of other components which, although not shown in any FIGS., would be readily understood by. . .

DETD . . . ASIC 20. Control of the adjustable gain IF receiver amplifier circuit 34 is accomplished by an automatic gain control circuit (**AGC**) 60. An **AGC** detector circuit 62 receives a representative IF signal through **AGC** input line 63. As is discussed in greater detail below, a direct current (DC) signal is output from the **AGC** detector circuit 62 through an **AGC** detector output line 64 which represents the strength of the received signal. An **AGC** integrator circuit 66 compares the DC signal to a relatively constant **AGC** reference signal received over an **AGC** reference line 67 from the MSM ASIC 22. The integrated difference between the two signals is output onto an open loop output

line 68 which is connected to a linear inverter 70 suppling an **AGC** control signal to the adjustable gain IF receiver amplifier circuit 34 over a receiver amplification control line 72. The linear.

.

.

DETD . . . the open loop output line 68 provides the open loop component of the total output power control so that the **AGC** integrator circuit 66 and **AGC** detector circuit 62 also contribute to open loop gain control. One of the functions of the negative summer circuit 80,. . .

DETD . . . onto the transmit gain adjust line 90 which is connected to the

negative summer 80 shown in FIG. 1. An **AGC** reference output 152 is also shown supplying the **AGC** reference signal onto the **AGC** reference line 67. The MSM ASIC 22 also includes a control bit (CB) 143 located in another area of MSM. . .

DETD The baseband ASIC 20 is shown supplying a representative receiver IF signal onto the **AGC** input line 63 through a receiver IF output (RX IF OUT) to the **AGC** detector 62. The representative receiver IF signal is examined by the **AGC** detector 62 to yield on the **AGC** detector output line 64 a DC representation of the received signal strength. A capacitor 170 blocks any DC component of the

signal on the **AGC** input line 63. Biasing elements 172, 174, 176, 178, and 180 are sized to bias a bipolar transistor 190 in. . . of the diode 204 is connected to a grounded resistor 206 and a resistor 210 which is connected to the **AGC** detector output line 64 along with a grounded capacitor 212. Since capacitor 200 is connected in

series (AC-coupled) with subsequent elements, capacitor 200 removes the DC component from the **AGC** input signal and cooperates with the diodes 202, 204 to add a new DC level to the AC component which. . . the remaining AC component to leave a DC signal which is linearly proportional to the AC signal level of the **AGC** input signal. In addition, the resistor 210 functions as an averaging means to slow the charge of capacitor 212 so that the **AGC** output signal on the **AGC** detector output line 64 is an averaged linear output. Furthermore, the resistors 206 and 210 are preferably approximately equal in. . .

DETD Refer now to FIG. 3 for a schematic view of the **AGC** integrator circuit 66, the linear inverter 70, and the negative summer 80. The **AGC** detector output line 64 is shown supplying signals through a biasing resistor 220 to the non-inverting input of an operational amplifier 222, which input is also connected to biasing components 220, 226, and 228. The **AGC** REF line 67 is shown providing the relatively constant **AGC** reference signal through a network of biasing elements 230, 232, 234, and 236 to the inverting input of the operational. . . gain control signal on the open loop output line 68 equal to the difference between the signal levels on the **AGC** detector output line 64 and the **AGC** REF line 67. The linear inverter 70 is shown receiving the gain control signal on the open loop output line. . .

=> d l5 3 pn

L5 ANSWER 3 OF 3 USPATFULL
PI US 5689815 19971118

```
 s (random number)(p)(cipher? or encipher? or encrypt? or cipher?)

        230435 RANDOM
       1620117 NUMBER
          8950 RANDOM NUMBER
                 (RANDOM(W)NUMBER)
          2770 CIPHER?
          1332 ENCIPHER?
         13890 ENCRYPT?
          2770 CIPHER?
L1        1548 (RANDOM NUMBER)(P)(CIPHER? OR ENCIPHER? OR ENCRYPT? OR CIPHER?)

=> s (wireless or cellular phone or wirless phone)(p)(l1)

         33234 WIRELESS
         92656 CELLULAR
         30181 PHONE
          5122 CELLULAR PHONE
                 (CELLULAR(W)PHONE)
            13 WIRLESS
         30181 PHONE
             0 WIRLESS PHONE
                 (WIRLESS(W)PHONE)
L2          41 (WIRELESS OR CELLULAR PHONE OR WIRLESS PHONE)(P)(L1)

=> d l2 41 kwic


L2   ANSWER 41 OF 41  USPATFULL
SUMM   Generally in such wireless pay TV systems, video signals and
       voice ignals are ciphered so as to be available to subscribers
       only, excluding others. A conventional example of those systems is
shown
       in FIG..  .  .  sent therefrom to an output terminal 2. At this time,
       the video signal polarity inverter 3 is controlled by a random
     number signal generator 4. That is, the video signal polarity
       inverter 3 produces an output but selectively inverting the polarity of
       the applied video signals in response to a logical value signal from
the
     random number signal generator 4, which value varies
       at random. A decoder is arranged to decode the ciphered video
       signals in accordance with a previously prepared key code signal so as,
       to reproduce a visible picture so that.  .  .


=> d l2 40 kwic


L2   ANSWER 40 OF 41  USPATFULL
AB     A method and apparatus is disclosed for providing a secure
     wireless communication link between a mobile nomadic device and
       a base computing unit. A mobile sends a host certificate (Cert.sub.--
       Mobile).  .  .  Cert.sub.-- Mobile is not valid, then the base unit
       rejects the connection attempt. The base then sends a Cert.sub.-- Base,
     random number (RN1) encrypted in mobile's
       public key and an identifier for the chosen SKCS to the mobile. The
base
       saves the RN1 value.  .  .  Pub.sub.-- Mobile, RN1 under the private
key
```

of the mobile. The mobile then generates RN2 and the session key, and **encrypts** RN2 under the Pub.sub.-- Base. The mobile sends the **encrypted** RN2 and E(Pub.sub.-- Mobile, RN1) to the base. The base then verifies the mobile signature using the Pub.sub.-- Mobile obtained. . . . key. The base then determines the session key. The mobile and base may then enter a data transfer phase using **encrypted** data which is decrypted using the session key which is RN1 .sym.RN2.

SUMM The present invention provides method and apparatus for providing a secure communication link between a mobile **wireless** data processing device and a base (fixed node) data processing device which is coupled to a network. The mobile sends. . . . CERT.sub.-- Mobile is not valid, then the base unit rejects the connection. attempt. The base then sends a CERT.sub.-- BASE, **random number** (RN1) and an identifier for the chosen SKCS to the mobile. The base saves the RN1 value and adds the. . . . RN1) under the private key of the mobile.

The mobile then generates RN2 and the session key (RN1O RN2), and **encrypts** RN2 under the Pub.sub.-- Base. The mobile sends the **encrypted** RN2 and E(Pub.sub.-- Mobile, RN1) to the base in a message signed with mobile's private key. The base then verifies. . . . The base then determines the session key (RN1.sym.RN2). The mobile and base may then enter a data transfer phase using **encrypted** data which is decrypted using the session key. The present invention further provides a method for changing the session key. . .

=> d l2 39 kwic

L2 ANSWER 39 OF 41 USPATFULL

DETD . . . intended remote location, initial contact must be established between master unit 400 and remote unit 450. For example, in a **cellular phone** system, this could be established when the sender of the call from remote unit 450 initially dials. and sends a.

. . for remote unit 450 as identified by its unique identification number. With SN1 and SN2 of the remote unit 450, **random number** generator 402 generates a **random number** R which is stored in R memory 404. **Random number** R is then sent from master unit 400 to remote unit 450 in which it is received and XOR-ed with SN1 at XOR gate 458. This XOR operation produces a first intermediate number A which is then **encrypted** by DES unit 456, using SN2 as the **encryption** key, to thereby generate a remote processed number RPN.

=> d l2 39 pn

L2 ANSWER 39 OF 41 USPATFULL

PI US 5517567 19960514

=> d l2 38 kwic

L2 ANSWER 38 OF 41 USPATFULL

DETD . . . key Knet (step 39). This may for example be performed by a conventional random generator simply generating Knet as a **random number**. The same Knet key shall be used for the whole network. The base station also computes the backbone key (Kb) to be used to **encrypt** security messages when they flow on the LAN backbone. Kb is derived from Knet. The **Wireless** Manager (network manager) is then triggered for starting a Kb retrieval process for further use

for next base or remote station installation (step 40). To that end, the **Wireless** Manager sends a first message (AUTH1) to the base station. Upon receiving said message, the base station generates a **random number** N1 (step 41) and sends it to the **Wireless** Manager (step 42) through a returning message (AUTH2). The **Wireless** Manager stores N1 and randomly generates a number N2 (steps 43 and 44). The network manager starts then generating an. . .

=> d l2 37 kwic

L2 ANSWER 37 OF 41 USPATFULL
DETD With the digital **wireless** telephone 80 described above, to select the primitive polynomial used in **encryption**, the primitive polynomial number is selected by means of a **random number** at the calling side, and the primitive polynomial number is transmitted to the called side. The selection of the primitive. . .

=> d l2 36 kwic

L2 ANSWER 36 OF 41 USPATFULL
SUMM A transmitting unit of a **wireless** security system generates randomized successive verification codes ("rolling verification codes"). In some embodiments, a pseudo-**random number** generator in the transmitting unit is used to generate a randomized synchronization code after power up which is transmitted to a receiving unit. The receiving unit uses information in the synchronization code to initialize a corresponding pseudo-**random number** generator in the receiving unit. The first verification code transmitted from the transmitting unit is generated by incrementing the transmitted pseudo-**random number** generator and **encrypting** and combining the output of the pseudo-**random number** generator with other information in accordance with a particular method. The receiving unit, in order to test the validity of the verification code received, increments its pseudo-**random number** generator and generates a corresponding "reference code" in accordance with the method used by the transmitting unit. If the reference. . . then the transmission is deemed a valid verification code. Successive verification codes are generated by successively incrementing the transmitting unit's pseudo-**random number** generator.

=> d l2 35 kwic

L2 ANSWER 35 OF 41 USPATFULL
DETD . . . fashioned from a private key of the security verification system 168 (FIG. 7) of the computer network 194, a large **random number**, and other identification information unique to the security verification system 168. Provided a substantially unobstructed signal path exists between the **wireless** transceiver device 64 (FIG. 3) of the computer terminal 60 and the **wireless** communication means 14 (FIG. 1) of a security badge 10, the security badge 10 will intercept, process, and be operable to return a part of the interrogation signal in a re-**encrypted** form (according to

the operation of the security badge 10 set forth in FIGS. 16A-16F, infra).